Information Governance for Health Research

Data Security Protection Toolkit Handbook

Document information	
Document name	Data Security Protection Toolkit Handbook
Author	Information Governance Officer
Version	V7.0
Issue date	25/06/2025
Approved by	FMS Information Governance for Health Research Group
Next review	30/07/2025

Document history

Version	Date	Summary of change
V1	21/10/2016	Version for Approval
V2	06/07/2017	Updated web links
V2	06/07/2017	Updated references to SIRO to Toolkit IRO
V3	2018	References to IGT changed to DSPT
V4	13/02/2020	Changes to Responsibilities and roles, referencing DPO Updates to Protecting confidentiality
V5	21/05/2021	Change references to FMS IGHR
V6	20/05/2022	Updated section on Data Incident, and data breach reporting.
V6.1	08/03/2024	Page 6 – Updated that NHS paper records should not be removed from the University. DSPT 1.3.12 Page 7 – Updated that public WIFI should not be used DSPT 6.3.2 Page 6 – Updated that the DPIA process should be followed. - DSPT 1.3.8
V6.2	12/03/2024	Page 6 – Updated guidance on paper records following the FMS IG Committee.

Printed on; 25 June 2025

V6.3	23/05/2025	Page 8 - Guidance on MFA added General updates to the toolkit following feedback from stakeholders.

Contents

Introduction

Department of Health and Social Care expect us to provide assurance that the University handle health and social care data appropriately. The Data Security Protection Toolkit is the method used by the Department of Health and Social Care for measuring the assurances on data management and security.

The purpose of this document is to provide toolkit members guidance on how to work within the requirements of the Data Security Protection Toolkit (DSPT).

The key words MUST, SHALL CONSIDER, REALLY SHALL NOT, OUGHT TO, WOULD PROBABLY, MAY WISH TO, COULD, POSSIBLE and MIGHT in this specification are to be interpreted as described in RFC 6919.

Roles and Responsibilities

Information Governance is everyone's responsibility. All staff contracts contain a clause that they are responsible for Data Protection and upholding confidentiality. The clause refers to the University Policy on Data Protection and states that breaching could result in disciplinary action.

Students obligations when they are undertaking research are explained in their Learning Agreement which states that they are exposed to confidential material they shall be required to sign 'Confidentiality Agreement'.

Key roles and responsibilities

Data Protection Officer (DPO)	Responsible for:- • Advise on the obligations under GDPR • To monitor compliance with regulation and data protection provisions and with policies of the University in election to the protection of personal data including the assignment of responsibilities awareness rising and training of staff involved in processing operations and the relating audits. • The data protection advances on risks associated with processing operations with account of the nature, scope, context and purposes of processing. • Signs off all Data Protection Impact Assessments
University Senior Information Risk Officer	Responsible for:- • Senior Information Risk Officer (SIRO) is a member of the University Executive with overall responsibility of data protection within the university. FMS Information Governance for Health Research group reports to SIRO via the DPO.
Research study Principal Investigator (PI) /	Responsible for:-

Information Asset Owner (IAO)	• Identifying Research Studies that need to be covered by the Toolkit and notifying the Toolkit Lead. The PI is responsible to ensure that all information provided is accurate. • Ensuring all Researchers in their Research Group undertake Information Governance and information security training. • Being accountable for their Research Study meeting the requirements of the toolkit within a timescale agreed between the PI and the IG Lead. • • Ensuring all Toolkit documentation is completed and kept up to date in line with any changes made to the study.
Researchers working on Toolkit registered Studies.	For each research study they have responsibility for:- ▪ Undertake online Information Governance and information security training. ▪ Running the "Does my Project need a Toolkit" checklist and if and Toolkit is required notifying the Information Governance Team. ▪ Sign the Toolkit Agreement (at the end of this document). ▪ Assisting in providing accurate information so that the Research Study/group can achieve its Toolkit.
Toolkit Information Risk Owner (TIRO)	The TIRO operates at an executive level and requires assurances that all relevant Information Governance processes, procedures and policies are in place. The TIRO takes ownership of the IG Framework and chairs the FMS IGHR.
Faculty Medical Sciences Information Governance for Health Research group	Provide expert advice and assurances to TIRO in respect of: • Changes in internal and external issues • Non-conformities and corrective actions • Monitoring and metrics • Audit results • Fulfilment of information security objectives • Feedback form interested parties • Management of risk • Oversight of effectiveness of the IG Framework • Continual improvement of the Information Security Management System (ISMS) The IG Steering Group's Terms of Reference are available on the Toolkit webpages. https://research.ncl.ac.uk/igfhr/contacts/fmsighrgroup/
Information Governance Officer	Provide expert advice to TIRO on data protection requirements
Information Governance Lead / Information Governance Officer (FMS)	Acts as the research IG interface between the TRO and FMS IGHR, providing expertise and facilitation. Primary contact for external interested parties. Takes day-to-day responsibility for the operation of all DSPT matters. Responsible for applications from researchers for NHS Digital data.

Senior Cyber Security Officer	Provide expert advice to TIRO and represent the University corporate Cyber security agenda.
NUIT support staff	Provide technical expertise in the various service areas that comprise the NHS Approved Storage; respond to incidents; develop services in response to emerging requirements, changes and non-conformities.

Training

As part of the NHS Toolkit all members **MUST** complete GDPR training every 12 months.

Staff (including honorary, guest and visiting) can access training at this link and follow the instructions below.

https://elements.ncl.ac.uk/login/index.php

1. Login with your usual NCL login details
2. Click on the 'Available Courses' which is the 1st box at the bottom of the screen
3. Click 'University Essentials'
4. Click 'Information Security (previously GDPR)"
5. You should then see an invitation to 'enrol me' click on this link
6. You should now see the GDPR online course option click on this
7. You can now 'start course'
8. The training included assessments of learning and understanding throughout. On completion of the training the system provides your certificate. Please download and keep this certificate.

PG Students access the online course materials through canvas please use the instructions below:

1. Go to https://canvas.ncl.ac.uk and Log In on the dashboard click NU Workplace Essentials Training

2. Click on GDPR Essentials and the training will start

If you have issues accessing Canvas, please contact the IT Service desk it.servicedesk@ncl.ac.uk for assistance.

Equivalent NHS Training

All members of the NHS are required to complete training every 12 months. If you are a NHS member of staff you can send us a copy of your certificate. The certificate must show your score and the date you passed the training.

Enrolment of a research project cannot be completed until all members for that research study have done the appropriate training. Project members who fail to complete training may be removed from the project and access to data removed.

Data Incidents

What is a Data Breach?

A personal data breach can be broadly defined as a data incident that has affected the confidentiality, integrity, or availability of personal data. In short, there will be a personal data breach whenever any personal data is accidentally lost, destroyed, corrupted, or disclosed; if someone accesses the data or passes it on without proper authorisation; or if the data is made unavailable and this unavailability has a significant negative effect on individuals.

Personal data breaches can include:

- access by an unauthorised third party.
- deliberate or accidental action (or inaction) by a controller or processor.
- sending personal data to an incorrect recipient.
- computing devices containing personal data being lost or stolen.
- alteration of personal data without permission; and
- loss of availability of personal data.

Responsibility

It is the responsibility of all Staff to report a data incident as defined above.

What do you do if you notice a Data Incident?

If you have Identified a possible data incident you MUST report it to the University via the Data Incidents Form no later than 24hrs after identifying the incident.

The Information Governance Team investigates the data incident and produces a report. Depending on the nature of the incident it may also involve the Cyber Security Team and any associated data processors.

The UK GDPR states that we must report to the ICO without undue delay but not later than 72 hours after becoming aware of it. The Information Governance team will report any data breaches.

Relevant Legislation;

- UK General Data Protection Regulation(UK GDPR)
- Data Protection Act 2018(DPA 2018)
- Common Law Duty of Confidentiality(CLDoC)

Data Incidents Involving Research Data

The Data incident MUST be reported to the University in all cases via the Data Incidents Form here as soon as possible. However, you will also need to inform the Research Sponsor and potentially the research funder.

Identifying and Minimising Risks to Personal Data

Any new project or change to an existing project must involve a risk assessment to ensure that all risks in relation to the access and to the processing of personal data are mitigated. This may involve completing a new Data Protection Impact Assessment (DPIA) or amending of an existing assessment.

Protecting Confidentiality

The following table identifies baseline security controls that are needed to reduce the risk of incidents that could detrimentally impact clinical data. Further additional security controls are also identified in the section Mobile Computing and Storage Devices, Data Sharing, Encryption, Data destruction/Deletion and WEEE, and Use of Third-Parties. These baseline security controls will be audited.

Ref	Risk	Control
	Clinical data is voluntarily disclosed by staff to unauthorised persons.	Access to clinical data is restricted on a strict 'need to know' basis.
		Do not discuss clinical data with anyone else who is not authorised to access that data.
		Do not discuss clinical data in public access areas such as trains, cafes, pubs, etc.
		Do not send clinical data through non-secure electronic messaging and publishing systems such as social media, instant messaging, online forums, web site comments, file/photo/video sharing, live audio/video streaming, podcasts, blogs, personal web sites, etc.
	Unauthorised persons enter work environments containing clinical data.	Challenge all unknown visitors who enter the work environment. Ask for their name; a form of ID; who invited them; and their reason for visiting. If they cannot provide this information, then immediately ask them to leave; also notify the University's Security Office.
		Access to buildings where toolkit research is carried out should be controlled access via this university smartcard access.
		All visitors sign-in and sign-out of the work environment. The logbook needs to record the date of visit; time of entry; time of exit; name of visitor; who they are visiting; and their reason for visiting.
		All staff and students wear University issued ID cards.
	Paper-based clinical data is viewed by unauthorised persons.	Adopt clear desk working practices so that clinical data is not left unattended on desks, cabinets, shelves, and printers.
		Securely store all paper-based clinical data in a locked filing cabinet, drawer or cupboard; and keep access codes and keys secure (e.g. stored in a PIN controlled safe or key cabinet in a room with restricted physical access controls). Paper based records should not be removed from University sites unless absolutely necessary. If any paper records are removed it should be secured while in transit in a locked briefcase, not left unattended, including in a parked car and the risks documented on

		the DPIA. Any paper based records that are removed from University sites should be returned without delay when they are no longer required.
	Electronic clinical data is viewed by unauthorised persons, when it is shown on computer display equipment.	Re-position computer display equipment so that clinical data cannot be viewed by unauthorised persons (e.g. does the screen face a ground floor window or a CCTV camera).
	Unauthorised access to IT systems containing clinical data.	Do not tell anyone your password. Avoid writing passwords down. If passwords are written down, then keep those passwords safe (e.g. kept in a locked drawer).
		Do not let anyone else use your computer account.
		Computers must have screensavers enabled and a lock screen enabled to gain access back into the machine.
		Never leave a logged-on computer unattended. Lock your computer if you are leaving for a short amount of time (e.g. coffee break). Log-off if you are leaving for longer periods (e.g. overnight, weekends, annual leave, etc.).
		Multi-factor authentication is to be used on all remotely accessible user accounts on all systems, with exceptions only as approved by the university board.
	Incorrect storage of clinical data on IT systems, making it accessible to the wrong people, and inaccessible to the correct people.	Store all clinical data on University provided restricted access shared network folders.
		Review network folder access permissions at least annually. Immediately revoke network folder access for staff who no longer require access to clinical data.
		Do not store clinical data on your personal home drive.
		Do not store clinical data on any personal computing or storage devices without authorisation from the Principal Investigator. Such authorisation needs to be provided based on a valid business reason and risk assessment.
		Do not store clinical data on any cloud-based computing service (e.g. Dropbox, OneDrive, iCloud, Google Drive, etc.).
	Clinical data is accidentally or deliberately destroyed.	Ensure clinical data is backed-up in fully on a regular basis.
	Clinical data is compromised or damaged by hackers.	Only use operating systems and software that is vendor supported and in receipt of the latest security updates.
		All computer equipment uses network should have configured software firewalls to block all untrusted in-bound network connections by IT staff.
		Disable all guest accounts and change all default passwords by IT staff.

		Public WIFI must not be used.
	Clinical data is compromised by malicious software.	All university devices will be centrally managed and setup by IT staff. They run anti-malware software and ensure software is in receipt of the latest vendor provided security updates and definition/signature file.
		Only install software obtained from trusted sources (e.g. obtained directly from the software vender or an approved reseller).

The risks and associated security controls contained in this document should not be regarded as comprehensive. It is inevitable that new risks will emerge as technology develops. You need to remain vigilant and ensure you do not engage in any activities that could place this data at risk. Everyone who is trusted to collect, store and/or process clinical data is responsible for its security.

Toolkit Data Storage

All data for a Toolkit registered project **MUST** be kept on the projects Toolkit Secure Storage. There will be a project drive setup at the start of DSPT/Enrolment. Access to the drive will only be granted after approval of the Project PI as approved by the Information Asset Owner (IAO) and the individual has successfully completed the IG training.

Toolkit data **MUST** not be stored on ANY cloud storage such as Microsoft Teams, OneDrive, or SharePoint.

The NHS Secure Storage **MUST** only be accessed via DSPT approved Desktops/Laptops (Endpoints). DSPT approved Endpoints are confirmed by your IT Staff and are secured in accordance with the Toolkit Information Security Policy.

Joiners and Leavers

All new members of the project team **MUST** be notified to the DSPT IG Lead, go through the University GDPR training and complete the agreement at the back of this document. They must also receive copies of all relevant documentation from the IG Lead. Please send an email to rec-man@ncl.ac.uk informing the IG lead of the new starter and which project they will be working on. The IG lead will then send the appropriate information to them.

When a member of the team leaves the DSPT IG Lead should be notified so that they can be removed from the member list. Access to the data **MUST** be removed as soon the member of the team leaves. If the member is changing organisations but will still be working on the project, then please notify the IG Lead so that appropriate arrangements can be made. This could include a Data Sharing Agreements with other organisations., and changes to agreements with NHS Digital and Ethical Review bodies.

Transfer of Personal and Confidential Material

All data transfers outside of the University **MUST** only occur where there is a valid Agreement in place. Agreements should be negotiated by Legal Services. All data transfers involving personal data require a completed DPIA.

The following methods must be used to transfer Personal Sensitive confidential data.

Transfer of Personally Identifiable data outside of UK

Certain types of data cannot leave the UK, data obtained from NHS Digital. These are Death Certificates, Birth Certificates and Cancer Registrations and information derived from these sources. These constraints are clearly identified within the Data Sharing Agreement with NHS Digital.

Data can only be transferred with the agreement of the Information Governance Officer(FMS) by the agreed method.

Mobile Computing & Storage Devices

Do not store any clinical data on any mobile computing or storage device, unless you are:

- Authorised to do so by the Principal Investigator; and
- That authorisation is based on a valid business case and risk assessment.

Mobile computing and storage devices refer to:

Computing devices	**Storage devices**
• Laptops • Tablets • Smartphones • Smartwatches • eBook readers • Digital pens • Augmented reality visors • Camera glasses	• External hard disk drives • USB flash drives • SD cards • CDs, DVDs, Blu-ray Discs • Magnetic tape

The above table should not be regarded as exhaustive. It is inevitable that new types of mobile computing and storage devices will be available to consumers in the future, and such devices may not be suitable for securely processing and storing clinical data.

If you are permitted to use mobile computing and storage devices, then you should submit a service request to NUIT for a securely configured device to be issued to you.

The key risks associated with mobile computing and storage devices include:

- A high monetary value makes them an attractive target for thieves;
- Their portable nature means can easily be lost or damaged;
- Some devices have cloud storage enabled by default, meaning that clinical data could be accidentally saved to a potentially unsecure IT service located in another country; and
- Many mobile devices have embedded technologies (i.e. camera, microphone, GPS, RFID, etc.) that can violate privacy, if they are activated by hackers or malicious software.

If you are permitted by your Principal Investigator to use mobile computing and storage devices to store and process clinical data, then the following controls need to be used to reduce the risk of that data being lost, damaged, or accessed by unauthorised people:

Risk	Control
Clinical data stored on the device is viewed by unauthorised persons.	Be aware of who can see your screen, especially if you are working in a public area (e.g. train, library, café, conference venue, etc.). If it isn't possible to position your screen to prevent unauthorised viewing, then do not access the clinical data stored on the device in public areas.
A device containing clinical data is lost or stolen.	Do not leave devices unattended in public or other non-secure locations (e.g. hotel room). If possible, anchor the device with an anti-theft cable to a secure fixture such as a radiator pipe. Be discreet when transporting devices. Don't not leave devices unattended in vehicles. Securely store devices in a locked drawer, cupboard, or safe.
	Turn on and enable device location capabilities (e.g. find my device), and remote device wiping, if these features are available.
	Encrypt the device using non-proprietary encryption algorithms in accordance with the DSPT Information Security Policy
	Protect the device with a password that is at least 8 characters long; is not based on a dictionary word; contains upper-cased and lower-case letters; and contains a mix of numeric and special characters. Do not disclose your password to anyone else.
	To prevent password guessing by unauthorised persons, certain devices will automatically lock or wipe a device after N number of incorrect logon attempts; this feature should be used if it is available.
	Only store clinical data on the device that is required for mobile working. Immediately delete that data from the device if it is no longer required for mobile working.
Clinical data stored on the device is permanently lost because the device is damaged, lost or stolen; or the data becomes corrupted.	Retain a master copy of all clinical data on secure University IT systems that are regularly backed-up.
Clinical data is accidentally saved to a non-secure cloud service located in another country.	Turn off cloud storage features built-in to mobile devices (e.g. cloud synchronisation). Uninstall all cloud storage software that might already be installed on the device.
Clinical data stored on the device is compromised or damaged by hackers or malicious software.	Run anti-malware software on the device. Ensure anti-malware software is still in receipt of the latest scanning engines, heuristics, and definition files / signatures. Configure anti-malware to perform a full system scan every day.

Clinical data stored on the device is compromised or damaged by hackers or malicious software.	Only use operating systems and applications that are still in receipt of vendor security updates. Ensure the latest security updates are installed.
	Run personal software firewalls on the device. Configure all software firewalls to block all untrusted in-bound network connections.
	Uninstall all unnecessary software
	Only install software obtained from trusted sources.
	Review application software permissions to ensure they are not excessive. For example, can applications turn on the camera, microphone, GPS and RFID features; can the applications make and receive phone calls; can the applications access your saved files and contacts list? If the answer is yes, then clinical data could be at risk of compromise.

Anonymization and Pseudo-anonymization

The ICO Anonymisation Code of Practice **must** be followed when using health and social care data.

ICO Anonymisation Code of Practice

Encryption

Encryption (cryptographic security) refers to the process of converting data into a form that cannot be understood by anyone who is not permitted to view that data. Encryption can be used to protect electronic clinical data in all forms, such as text, audio, video, executable code, etc.

Without encryption, it becomes a relatively simple task for criminals to intercept, access, and modify clinical data when it is:

- Sent across the Internet or other untrusted network (e.g. as an email attachment); and
- Stored on portable computing and storage devices (e.g. laptops, tablets, smartphones, USB flash drives, external hard disk drives, etc.).

The following cryptographic controls need to be used to reduce the risk of clinical data being accessed and compromised by unauthorised people; and to ensure encrypted clinical data can be recovered in the event of a disaster:

Risk	**Control**
Clinical data is Intercepted, accessed, and/or modified by unauthorised persons when sent across the Internet; or when stored on portable computing or storage devices.	Encrypt clinical data using only non-proprietary encryption algorithms that are proven to be secure, such as AES 256 bit or stronger. Use long encryption keys or passphrases to encrypt clinical data (e.g. use long sentences rather than individual words). Keep encryption keys or passphrases secure. Never store or transmit encrypted clinical data with its encryption key or passphrase.

Encryption products contain security vulnerabilities that may result in compromise of encrypted clinical data and/or compromise of encryption keys and passphrases.	Use only encryption products that have been verified as secure by recognised authorities (e.g. encryption products certified as compliant with FIPS140-2, etc.). Use only encryption products that are still vendor supported and have the latest security updates installed.
Encryption keys and passphrases are compromised as a result of human error or technical vulnerability.	Immediately stop using compromised encryption keys and passphrases. Create replacement encryption keys and passphrases. Use a suitably secure communications channel to distribute replacement encryption keys and passphrases to authorised recipients (e.g. telephone voice call, SMS text message, special delivery letter, etc.).
Encryption keys and passphrases are lost, making it impossible to revert encryption.	Store all clinical data in an unencrypted form on the University's secure IT infrastructure (e.g. a secure shared network folder that can only be accessed by your team).

Data Destruction/Deletion

Many data incidents reported in the news have been attributed to poor disposal of data, including:

- Sensitive written and printed data being discovered in recycling plants;
- Large volumes of sensitive data being kept in non-secure storage, sometimes in abandoned buildings, and subsequently forgotten about;
- Filing cabinets and IT equipment containing sensitive data sold on the Internet; and
- Security research groups have used freely available software to reconstruct previously deleted data from hard disk drives bought off the Internet.

The following table summarises the risks that can occur when disposing of clinical data, and the controls that need to be used to reduce that risk:

Risk	**Control**
Reconstruction of paper documents after destruction.	Use a DIN 66399 Level 4 or higher cross cut shredder. Destroy large volumes of printed material by using the University's secure waste disposal bag service.
Recovery of video and audio tape recordings of clinical data.	Degauss all video and audio tapes containing clinical data.
Reconstruction of previously deleted data stored on removable media. ***Note:*** *Removable media refers to floppy disks; Zip disks; Jaz disks; magnetic tape; SD cards; USB flash drives; etc.*	All of these devices, and their variants, need to be need to be destroyed by the University's contracted data destruction company in compliance with the "Sustainable Campus" initiative - https://www.ncl.ac.uk/sustainable-campus/themes/waste-and-recycling/recycle/#d.en.902732

Inability to delete data from optical media such as CDs, DVDs and Blu-Ray discs.	Use a shredder that reduces optical media to small particles rather than strips. Destroy large volumes of optical media by using the University's contracted data destruction company.
Reconstruction of previously deleted data stored on Hard Disk Drives (HDDs).	If a HDD is to be re-used within the University, then all clinical data stored on that HDD will need to be securely deleted using software tools that satisfy NHS data destruction requirements; or be subject to degaussing. If the HDD is subject to physical disposal, then it will need to be destroyed by the University's contracted data destruction company.
Reconstruction of previously deleted data stored on Solid State Disk Drives (SSDs). ***Note:*** *Many secure deletion tools are ineffective on SSDs.*	Do not store clinical data on devices containing SSDs. If clinical data is stored on devices containing SSDs, then those SSDs need to be removed from the device and physically destroyed by the University's contracted data destruction company. If SSDs cannot be removed (e.g. they are surface mounted directly onto the logic board) as is the case with tablets and smartphones, then the entire device will need to be destroyed at the end of its functional life by the University's contracted data destruction company in compliance with the "Sustainable Campus" initiative. Do not donate these devices to charitable organisations for reuse outside the University. Certificates of data destruction need to be obtained and kept on record for at least 7 years.
It is not known if adequate destruction techniques were used when disposing of clinical data.	Keep a record of all discarded media that contains clinical data. Include: date of disposal; authorisation for disposal; methods of destruction; who carried out the destruction; and if a certificate was obtained for the destruction.

Use of Third Parties

Third-parties, if they are used to collect, provide, store and/or process clinical data on behalf of the University, should be subject to adequate contractual controls that reduce the impact and likelihood of serious data incidents. The following table identifies risks associated with third-parties, and the types of contractual controls that need to be used to manage that risk:

Risk	**Control**
Clinical data is compromised as a result of a third-party, or other sub-contractor, not having adequate information security controls.	Third-party MUST complete a SISA to confirm that they can provide adequate procedural and technological controls to safeguard clinical data. For example, does the third-party offer: • Adequate information security policies that have been disseminated to all third-party staff? • A data processing environment that has been independently certified as compliant against recognised information security standards such as ISO/IEC27001:2018?

	• Staff that have been subject to appropriate background security checks? • Basic physical security such as offices and data centres that are alarmed and monitored by CCTV, with access restricted to authorised personnel only? • Basic technological controls such as: a network perimeter firewall that blocks all untrusted in-bound Internet traffic; IT systems that are hardened in compliance with vendor recommendations; vendor supported operating systems and applications that are in receipt of the latest security updates; vendor supported anti-malware software that is in receipt of the latest definition/signature files, etc.? • Basic technological controls that have been independently audited against recognised cybersecurity standards such as HM Government's Cyber Essentials Plus scheme? • IT infrastructure and web applications that have been subject to quarterly vulnerability scanning and annual penetration testing by suitably qualified persons (e.g. CREST, Tiger Scheme)? • Adequate data disposal mechanisms that render recovery of clinical data impossible? The third-party needs to declare any other parties (i.e. sub-contractors) that will be used to collect, store and/or process clinical data. The third-party also needs to declare the types of due diligence performed against those other parties.
Security incidents involving clinical data are not notified to the University by the third-party.	Ensure the third-party provides the University with immediate notification of all security incidents involving clinical data and needs to be contained within the contract Data Sharing Agreement. The incident should be reported via the data breach notification form.
Clinical data is exported to countries that do not have adequate data protection laws.	Perform due diligence against the third-party to confirm that they will not export clinical data outside the European Economic Area (EEA). Ask the third-party to provide postal addresses of all sites where clinical data will be located.
Clinical data cannot be accessed because of third-party IT system failure.	Ensure the third-party provides appropriate IT Service Level Agreements that are within acceptable tolerances (e.g. will it be minutes, hours, days or weeks before the IT service is restored?).
Clinical data is destroyed in the event of a disaster.	Perform due diligence against the third-party to confirm that they have adequate Disaster Recovery/Business Continuity Planning (DR/BCP) arrangements in place that are independently certified as compliant against recognised DR/BCP standards such as ISO22301:2012.
The third-party ceases to exist rendering clinical data inaccessible.	Make sure that the Third Party as part of their agreement has obligations which they would need to meet.
Clinical data cannot be returned in a usable form because the third-	Ensure the third-party uses only open non-proprietary methods of data encoding, so that clinical data can be retrieved by the University and processed on University IT systems.

party uses proprietary data encoding (e.g. data lock in).	
Clinical data remains on third-party IT systems after the University ends its relationship with the third-party.	Ensure that contracts with third parties specify deletion at the end of the contract.
The third-party does not put in place, or fails to maintain, the required security controls.	Ensure that you have the right to conduct on-site and off-site audits of the third-party's information security arrangements.
	Ensure that you have the right to instruct the third-party to carry out remedial security work, at their own cost, if their security controls are not adequate.
	Ensure that you have the right to request the immediate secure return of clinical data to the University, and the immediate secure disposal of clinical data from third-party systems, if there is a continued failure by the third-party to put in place adequate security.

Third Party Contracts should be negotiated by the relevant University section.

- Grants and Contracts
- Legal Services
- Procurement

Monitoring and Auditing

All members of the Toolkit will be monitored and audited to make sure that they are complying with the Information Governance Statement, the DSPT Handbook and the DSPT Information Security Policy. This is documented within the Data Security Audit Checklist which is a self-assessment completed by PI's and reviewed by the Information Governance Team.

Related University Policies and Procedures

Information Security Policy

Research Data Management Policy

Data Protection Policy and Guidance

Records Management Policy and Guidance

Information Security Guidance

Links to Further Guidance

Data Management Plan

DSPT Website

DSPT Documentation

ICO Guidance is extensive and an invaluable source of information.

NHS Guidance

Code of Practice on Confidential information

Anonymisation Standard for Publishing Health and Social Care Data: https://digital.nhs.uk/data-and-information/information-standards/information-standards-and-data-collections-including-extractions/publications-and-notifications/standards-and-collections/isb1523-anonymisation-standard-for-publishing-health-and-social-care-data

Office of National Statistics (ONS) Guidance for Birth and Death Statistics

Appendix 1 Agreement

All staff/students who are part of the DSPT **MUST** agree to follow the guidance in this Handbook.

I, _____, hereby acknowledge and declare that:
Print Name

(i) I am aware that policies are available to me on the intranet/in this handbook, or upon request to rec-man@ncl.ac.uk It is my responsibility to familiarize myself with these policies.

(ii) In addition, I confirm that I have received, read and understood the following:
a. DSPT Information Governance Statement
b. DSPT Handbook
c. DSPT Information Security Policy

(iii) I agree to conduct my activities in accordance with the University policies and understand that breaching these standards may result in disciplinary action up to and including termination or other legal remedy available to the organization.

(iv) I agree to undertake all the training that is required as documented within this document.

Signed:_____

Date:_____

Appendix 2 Glossary

DSPT	Data Security Protection Toolkit
FMS IGSG	Faculty of Medical Sciences, Information Governance Steering Group
TIRO	Toolkit Information Risk Officer
Information Asset Owner (IAO)	The Information Asset owner is responsible for the Information Asset that they are an owner of.
Information Asset	An information asset is a body of information, defined and managed as a single unit so it can be understood, shared, protected and exploited effectively. Information assets have recognisable and manageable value, risk, content and lifecycles.
FMS IG Framework	The information management system which the university uses to delivers IGT.
Toolkit Members	List of everyone involved in the IGT
Endpoint	The device that you access the data through. Desktop, Laptop, Tablet, other device.
Confidentiality Agreements	A type of agreement / contract between two or more parties which sets out conditions of accountability and confidentiality.
Data Sharing Agreements	A type of agreement/contract which set out the conditions of what data is shared and under what circumstances, these agreements usually also
PID	Personal Identifiable Data
PVC	Pro Vice Chancellor
ICO	Information Commissioner Office